Inside China’s controversial mission to reinvent the internet

Huawei is developing the technology for a new network. But what does this mean for the rights of users?

yesterday

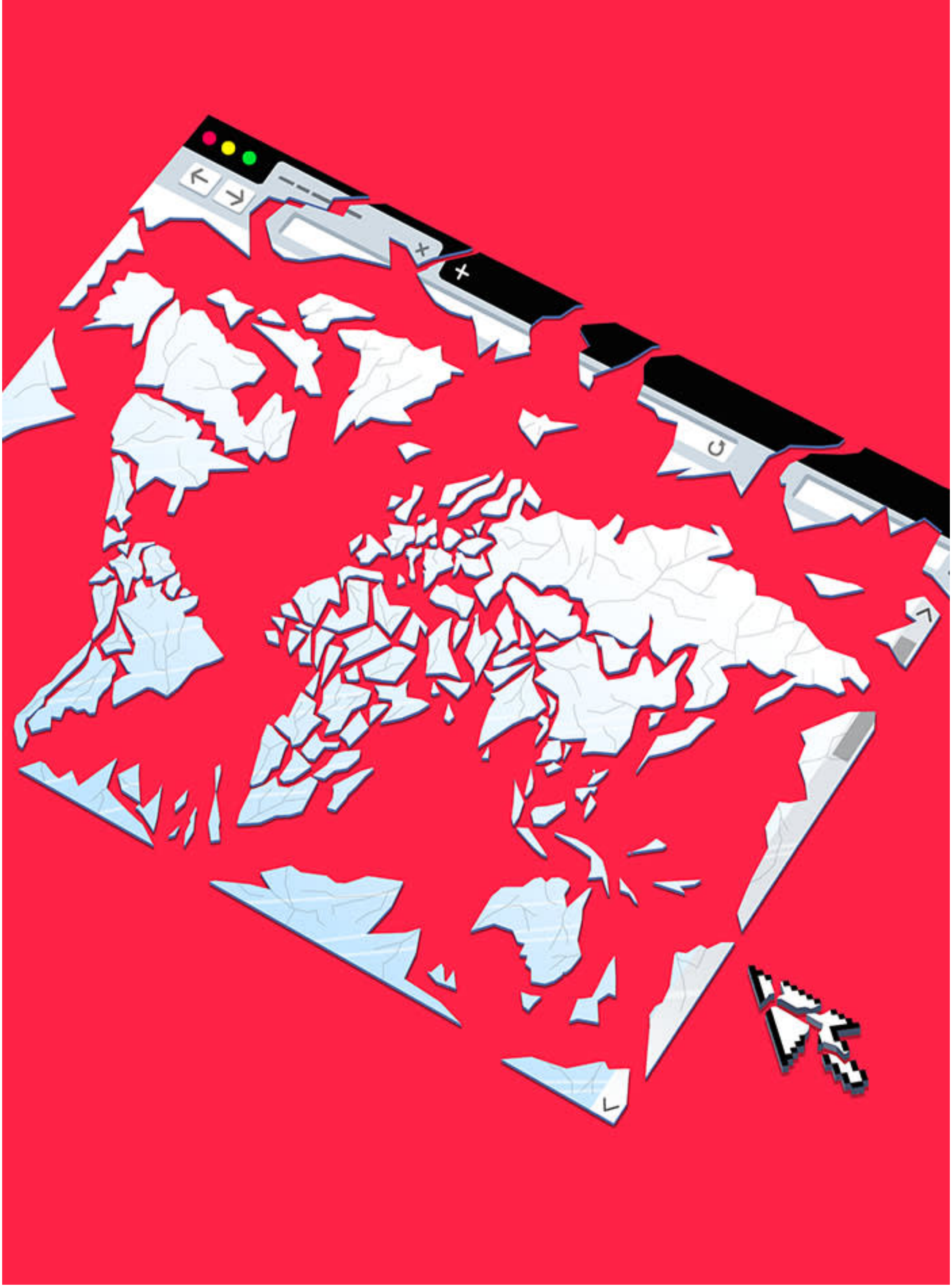
On a cool day late last September, half a dozen Chinese engineers walked into a conference room in the heart of Geneva’s UN district with a radical idea. They had one hour to persuade delegates from more than 40 countries of their vision: an alternative form of the internet, to replace the technological architecture that has underpinned the web for half a century.

Whereas today’s internet is owned by everyone and no one, they were in the process of building something very different — a new infrastructure that could put power back in the hands of nation states, instead of individuals.

The team who had masterminded the New IP (internet protocol) proposal was from the Chinese telecoms giant Huawei, which had sent the largest delegation of any company to the September meeting.

At the gathering, held at the International Telecommunications Union, a UN agency that establishes common global standards for technologies, they presented a simple PowerPoint. It didn’t bother with much detail on how this new network would work, or what specific problem it was solving. Instead, it was peppered with images of futuristic technologies, from life-size holograms to self-driving cars.

The idea was to illustrate that the current internet is a relic that has reached the limits of its technical prowess. It was time, Huawei proposed, for a new global network with a top-down design, and the Chinese should be the ones to build it.



The New IP proposal could embed a system of centralised rule enforcement into the technical fabric of the internet. Saudi Arabia, Iran and Russia have previously shown support for Chinese proposals for alternative network technologies © Alexander Glandien

Governments everywhere seem to agree that today's

model of internet governance — essentially, lawless self-regulation by private, mostly American companies — is broken.

New IP is the latest in a series of efforts to change the way the internet is run, spearheaded by governments that were largely left out when it was founded half a century ago. “The conflicts surrounding internet governance are the new spaces where political and economic power are unfolding in the 21st century,” wrote the academic Laura DeNardis in her 2014 book *The Global War for Internet Governance*.

The Chinese government in particular has viewed designing internet infrastructure and standards as core to its digital foreign policy, and its censorship tools as proof-of-concept for a more efficient internet, to be exported elsewhere.

“Of course [China] want a technological infrastructure that gives them the absolute control which they have achieved politically, a design that matches the totalitarian impulse,’’ says Shoshana Zuboff, author of *The Age of Surveillance Capitalism* and a social scientist at Harvard University. “So that is frightening to me and it should be frightening to every single person.”

Huawei claims that New IP is being developed purely to meet the technical requirements of a rapidly evolving digital world, and that it has not yet baked a particular governance model into its design. The telecoms giant is leading an ITU group that is focused on future network technology needed by the year 2030, and New IP is being tailored to meet those demands, a spokesperson says.

What is known about the proposal has come primarily through two jargon-filled documents that have been shared with the FT. These were presented behind closed doors to ITU delegates last September and this February. One is a technical standards proposal, and the other a PowerPoint titled "New IP: Shaping the Future Network".

The ITU's headquarters in Geneva, where Huawei representatives presented ideas for a new top-down internet protocol. Parts of the technology may be ready to be tested by next year © Getty

Despite the might of today's internet, it has no regulator; instead, power is largely held by a handful of US corporations — Apple, Google, Amazon, Facebook. This lack of central oversight is the very thing that has allowed technologists to transform how we communicate and live but it has also enabled deep fractures in our social order, including the manipulation of public dialogue, the disruption of democracy and the rise of online surveillance.

Today, in the wake of scandals from Cambridge Analytica to the role of Facebook in inciting real-world violence in Myanmar, many experts see the internet as a civic space that requires better public hygiene. Governments — whether democratic or authoritarian — are tired of being shut out and are agitating for more influence online.

The power balance is starting to shift but the scope of what states want varies widely. The US, UK and Europe, for example, are interested in adapting the current system to introduce more regulatory power, and give intelligence agencies greater access to users' personal data.

The Chinese New IP proposal is far more radical, and could embed a system of centralised rule enforcement into the technical fabric of the internet. Saudi Arabia, Iran and Russia have previously shown support for Chinese proposals for alternative network technologies, according to sources who were present at ITU meetings. The proposals revealed that the blueprints for this new network have already been drawn up, and construction is under way. Any country will be free to adopt it.

“Right now we have two versions of the internet — a market-led capitalist version based on surveillance, which is exploitative; and an authoritarian version also based on surveillance,” Zuboff says. “The question is: will Europe and North America pull together to construct the legal and technological frameworks for a democratic alternative?”

The New IP presentation paints a picture of a digital world in 2030 where virtual reality, holographic communication and remote surgery are ubiquitous — and for which our current network is unfit. Traditional IP protocol is described as “unstable” and “vastly insufficient”, with “lots of security, reliability and configuration problems”.

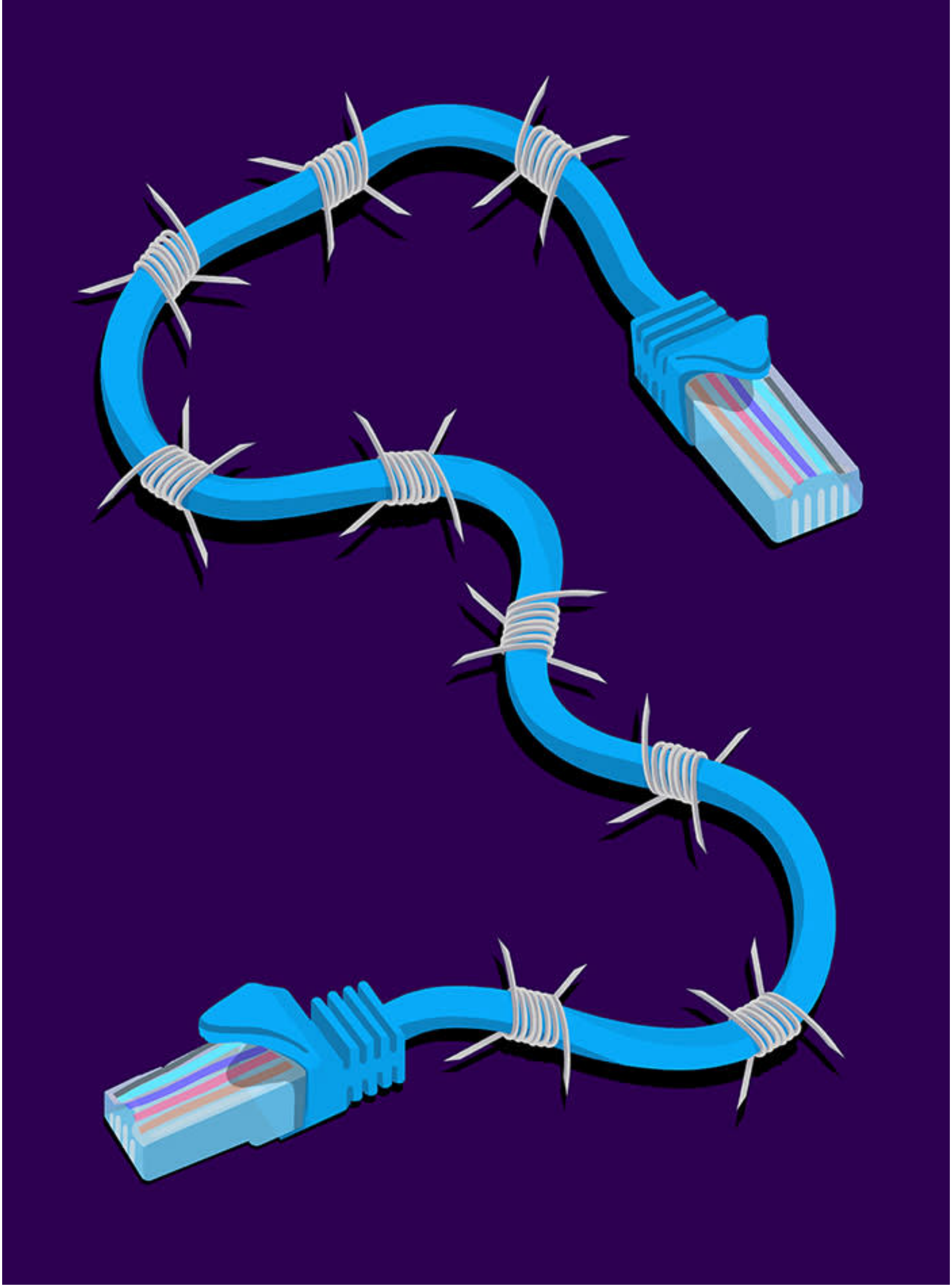
The documents suggest a new network should instead have a “top-to-bottom design” and promote data-sharing schemes across governments “thereby serving AI, Big Data and all kinds of other applications”. Many experts fear that under New IP, internet service providers, usually state-owned, would have control and oversight of every device connected to the network and be able to monitor and gate individual access.

The system is already being built by engineers from “industry and academia” across “multiple countries”, Huawei’s team lead Sheng Jiang told the group in

September, although he would not reveal who these were due to commercial sensitivities. Among the audience were veterans of the ITU, including mainly government representatives from the UK, the US, Netherlands, Russia, Iran, Saudi Arabia and China.

For some participants, the very idea is anathema. If New IP was legitimised by the ITU, state operators would be able to choose to implement a western internet or a Chinese one, they say. The latter could mean that everyone in those countries would need permission from their internet provider to do anything via the internet — whether downloading an app or accessing a site — and administrators could have the power to deny access on a whim.

Rather than a unified world wide web, citizens could be forced to connect to a patchwork of national internets, each with its own rules — a concept known in China as cyber sovereignty.



During recent periods of civil unrest, Iran and Saudi Arabia blacked out internet connectivity for prolonged periods, except for certain 'essential' services © Alexander Glandien

Recent events in Iran and Saudi Arabia provide a glimpse of what this would look like. These governments blacked out global internet connectivity for prolonged periods during civil unrest, allowing only restricted access to essential services such as banking or healthcare. In Russia, a new “sovereign internet” law passed in November enshrined the government’s right to monitor web traffic closely and showed the country’s capability to cleave off from the global web — a capability that Chinese companies including Huawei helped the Russians build.

Experts now debate whether China’s vision of its internet governance may be shifting from a defensive one, in which the government wished to be left alone to impose authoritarian internet controls at home, to a more assertive approach, in which the country is openly advocating for others to follow its lead.

The creators of New IP say that parts of the technology will be ready to be tested by next year. Efforts to persuade delegations of its value will culminate at a major ITU conference due to be held in India in November. To persuade the ITU to approve it within the year, so it can be officially “standardised”, representatives must reach an internal consensus, based loosely on majority agreement. If the delegates are unable to agree, the proposal will go to a closed-door vote in which only member countries can participate, cutting out the views of industry and civil society.

This rapid timeline is causing western delegations particular anxiety and demands have been made to slow the process down, according to documents seen by the FT. One participant from the Dutch delegation wrote in an official response, leaked to the FT by multiple sources, that the "open and adaptable nature" of the internet — both its technical structure and how it is governed — was fundamental to its success and that he was "especially concerned" that this model veered away from that philosophy.

Another stinging rebuke from a UK delegate, also leaked to the FT, declared: "It is far from clear that technically sound justifications have been made for taking such a radical step. Unless these are forthcoming, reasonable foundations for future work or even continued research activities on these topics are either weak at best, or nonexistent."

One of the loudest critics of New IP has been Patrik Fältström, a long-haired maverick engineer, known in his native Sweden as one of the fathers of the internet. In the early 1980s, Fältström was a mathematics student in Stockholm when he was hired to build and test the infrastructure for a new technology that the US government was calling the internet.

His job was to write a series of protocols that allowed computers to send text between each other. "In Europe, we were maybe 100 people in Sweden, 100 in the UK, 50 here, 20 there, all of us knew each other. We used to joke that if there was a problem, you knew who to call," he says.

Today, Fältström is a digital adviser to the Swedish government and its representative at most major internet standards bodies including the ITU. Thirty years after he helped assemble the building blocks of the internet, he embodies the cyber-libertarian western ideals that were woven into its foundation.

"Internet architecture makes it very, very hard, almost impossible for whoever is providing internet access to know or regulate what the internet access is used for," he says. "That is a problem for law enforcement and others, who would like to have an internet service provider controlling it, so it is not used for illegal activities like pirating movies, or child abuse.

"But I am prepared to accept that there will be criminals who do bad things and police will have an inability to fight [all of] it. I accept that sacrifice."

For Fältström, the beauty of the internet is its "permissionless" nature, as demonstrated during the Arab spring. "We have to remember," he says, "it is a balance between being able to communicate and control, but people having a voice is always more important."

A stark contrast to this view can be found in a river-village called Wuzhen near Shanghai, which is emptied out every autumn to make room for the tech executives, academics and policymakers attending the ambitiously named World Internet Conference. The event was created by the Cyberspace Administration of China in 2014, a year after President Xi Jinping rose to power. A row of world flags greets visitors — a nod to Xi's vision of creating "a community of shared future in cyberspace".

Tim Cook, CEO of Apple, at China's World Internet Conference in 2017. In recent years, foreign attendance has dropped off as the US-China tech war intensified and executives worried about being too aligned with Beijing © Getty

Tech executives from Apple's Tim Cook to Qualcomm's Steve Mollenkopf have spoken there, lending credence to Xi's attempts to assemble the international tech elite. But in recent years, foreign attendance has dropped off as the US-China tech war intensifies and executives worry about being too closely aligned with Beijing.

There is precedent for such fears. In the event's first year, organisers slipped a draft joint statement under guests' hotel doors at midnight, setting out Xi's view of each nation's right to "cyber sovereignty". Guests were told to get back with any changes before 8am. After protests, the organisers dropped the matter entirely. But the fact that the leadership had tried such a stunt reflected Xi's digital ambitions.

In the early 1990s, the Chinese government started developing what is now known as the Great Firewall, a system of internet controls that stops citizens from connecting to banned foreign websites — from Google to The New York Times — as well as blocking politically sensitive domestic content and preventing mass organising online.

Beijing's technical controls are supported by large teams of government censors as well as those hired by private tech companies such as Baidu and Tencent. Although anyone anywhere in the world can technically host their own website using just a computer and an internet connection, in China one needs to apply for a licence to do so. Telecoms providers and internet platforms are also required to aid the police with the surveillance of "crimes", which can include actions such as calling Xi a "steamed bun" in a private chat group, an act punished by two years in prison.

Chinese President Xi Jinping at the World Internet Conference in 2015, where he told attendees that every nation should have independent authority over its own internet © Getty

Despite this, the Chinese internet is not 100 per cent effective at blocking content considered sensitive or dangerous by the government. "The leaky global internet remains frustrating for Chinese censors, and they've dealt with it at great expense and effort, but if you could make those problems go away almost completely by using a more automated and technical process, perhaps like New IP, that would be fantastic for them," says James Griffiths, author of *The Great Firewall of China: How to Build and Control an Alternative Version of the Internet*.

"Building a new version of the internet would potentially block more people from gaining politically dangerous knowledge, saving a huge amount of effort, money and manpower from the censorship side. They can pick and choose what controls they want, bake it into the tech and roll it out."

Establishing a sophisticated alternative to the western internet would also fit with China's ambitions to extend its digital footprint globally. "In the early days of the internet, China was very much a follower and didn't recognise, like many other countries, how disruptive the internet would be," says Julia Voo, research director for the China Cyber Policy Initiative at Harvard University's Belfer Center.

"As they realised how important it was, [they] funnelled more resources into developing technologies . . . and we can see their increased influence in many standards organisations like the ITU in the past two or three years.

"But the US and others have made a strategic mistake in not seeing the value of growing infrastructure in developing markets," she adds. "There is still a lot of infrastructure that needs to be provided and in the past 10 years it has been Chinese companies that have been the ones to provide it, particularly in Africa."

Beijing has signed memoranda of understanding on building a "Digital Silk Road" — or system of advanced IT infrastructure — with 16 countries. Huawei says it has 91 contracts to provide 5G wireless telecoms equipment worldwide, including 47 from Europe — despite US warnings that Huawei's involvement was tantamount to giving the Chinese access to national security secrets, an allegation rejected by the company.

“In proving that you can control and intensely surveil your domestic internet and avoid it being used as a tool to rally people against the government, combined with the economic success of its companies, China has made this vision incredibly attractive to regimes — autocratic and otherwise — around the world,” says Griffiths.

The ITU was created 155 years ago, making it one of the oldest international organisations in the world, predating even the UN. It is housed in a set of glass-panelled buildings in Geneva’s Place des Nations. On the 10th floor of one is the airy office of Bilel Jamoussi, the Tunisian-born head of the ITU’s study groups — the units that develop and ratify technical standards.

The room is lined with an enormous bookcase from which Jamoussi pulls a dusty blue book — his PhD thesis, penned 25 years ago, about traffic going through the internet. At the time, there was a desire to build a new networking protocol to meet the internet’s growing user base. In the end engineers opted to layer on top of the existing TCP/IP infrastructure. The technology, invented in the late 1970s by computational engineers working for the US defence department, was a way of transmitting messages between computers at the speed of light, using a special addressing system.

Bilel Jamoussi, head of the ITU's study groups, which ratify technical standards. 'Twenty years ago it was Europe and North America that were dominating the products, solutions and standards development, now we have a swing to the east' © YouTube

"Twenty-five years ago we had this conversation as a community — is it TCP/IP or is it something else — and then a lot of design and development happened to kind of rescue [it]," Jamoussi says. "We are now, I think, at another turning point, of saying, is that enough, or do we need something new?"

In its earliest days, the ITU oversaw the first international telegraph networks. Since then, it has grown from 40 nations to 193 and has become the de facto standards body for telecoms networks. Standards produced there legitimise new technologies and systems in the eyes of certain governments — particularly those in the developing world who don't participate in other internet bodies. Ultimately, they give a commercial edge to the companies who have built the tech they are based upon.

Over the past 21 years, Jamoussi has witnessed a geopolitical shift. “The pendulum has swung to the east, and now we see more participation from China, Japan, Korea,” he says. “Twenty years ago it was Europe and North America that were dominating the products, solutions and standards development, now we have a swing to the east.”

On one of the ITU’s marble walls, backlit flags are hung, showing the biggest donor nations. The Chinese flag — currently at number five — was not there at all a few years ago, an employee explained, but it has been gradually working its way up.

New IP is the latest grenade thrown into the ITU’s arena, but it is hardly the first internet-related standard to be proposed as an alternative to the original western-designed system. The governments of Russia, Saudi Arabia, China and Iran have been pushing the idea of alternative networks for years, according to participants who wished to remain anonymous.

“In the early 2000s, once you saw widespread take-up of the internet, suddenly you had this idea of democratisation, of essentially giving people more control and more information. For authoritarian governments, that was something they weren’t happy with,” says one member of the UK delegation. “And so work started, around the early 2000s, particularly in China, and then a bit later in Iran and Russia, around how to create an alternative to the standards and the technologies that were being developed mostly by Americans still."

But in recent years, Chinese companies have moved on to New IP. "There's a new paradigm, it's not voice and text and video and people chatting, it's the real-time controlling of something remotely, or having telepresence, or holograms," Jamoussi explains. "Those new applications are requiring new solutions. And now it's more feasible, it's no longer science fiction, it's close to being a reality."

Spearheading plans for New IP is Richard Li, chief scientist at Futurewei, Huawei's R&D arm located in California. Li has been working with Huawei engineers based in China, as well as state telecoms companies China Mobile and China Unicom, with the explicit backing of the Chinese government, to develop the technology specifications and standards proposal.

Having Huawei at the helm will ring alarm bells for many in Europe and the US, where governments have become concerned that Chinese technology is being developed as a vehicle for state espionage. The advent of 5G — a much higher bandwidth network which will serve as the digital spine for a more automated world — has led to rising concern that products developed by Huawei will be built with "back doors" for spies in Beijing.

Richard Li, chief scientist at Futurewei, Huawei's R&D arm. Li has been working with the explicit backing of the Chinese government to develop the technology that would allow 'cyber sovereignty' © YouTube

Last year, the US blacklisted Huawei from selling into its market, and the UK government is embroiled in a parliamentary battle over the company's involvement in its core telecoms infrastructure.

The FT reached out to Li to discuss New IP, but Huawei declined the opportunity for him to explain the idea in greater detail. The company said in a statement: "New IP aims to provide new IP technology solutions that can support . . . future applications such as Internet of Everything, holographic communications, and telemedicine. The research and innovation of New IP is open to scientists and engineers worldwide to participate in and contribute to."

Critics argue that the technical claims made in the New IP documentation are either false or unclear, and represent a “solution looking for a problem”. They insist that the current IP system is fit for purpose, even in a rapidly digitising world. “The way that the internet has developed is through building blocks that are modular and loosely coupled, that’s the brilliance of it,” says Alissa Cooper, chair of the Internet Engineering Task Force (IETF), an industry-dominated standards body in the US.

In November, Li presented to a small group during an IETF meeting in Singapore, which Cooper attended. “[The current infrastructure] is in pretty stark contrast to what you see in the New IP proposal, which is this kind of monolithic, top-down architecture that wants to tightly couple the applications to the network. This is exactly what the internet was designed not to be,” she says.

The implications for the average user could be enormous. “You’re pushing control into the hands of [telecoms] operators which are state-run,” says a UK ITU delegation member. “So [it means] you can now not only control access to certain types of content online, or track that content online, but you can actually control the access of a device to a network.”

For internet pioneer Patrik Fältström, the beauty of the internet is its ‘permissionless’ nature. ‘We have to remember,’ he says, ‘it is a balance between being able to communicate and control, but people having a voice is always more important’ © Alexander Glandien

China is already in the process of building a credit-scoring system for its population, based on online and offline behaviour and past “misdemeanours”, the delegation member noted. “So if somebody’s social credit score dipped below a certain amount because they were posting on social media too much, you could actually prevent that phone from connecting to the network.”

China’s telecoms operators have a wealth of data on their subscribers. By law, customers have to register for a phone number or internet connection using their real name and identification, which is then accessible by other companies such as banks. The country's cyber-security law also mandates that all "network operators", which includes telecoms companies, must keep "internet logs" — although it is not clear what these entail.

Jamoussi argues it is not the ITU's place to judge whether proposals for a new internet architecture are "top-down'" or could be misused by authoritarian governments. "Of course anything you build, it's a two-edged sword. You can use anything for good or for bad, and it's the sovereign decision of every member state," he says. "In the ITU we don't go into that potential misuse of technology, we just focus on, 'here is some . . . communication technology problem, here is an aspiration, let's as a community build a solution to reach that.' But then how people use it is really up to them."

Beijing's ambitions to build more controls into the internet infrastructure are not seen as a problem by everybody — merely as the next chapter in its evolution.

"The internet was supposed to be a neutral infrastructure, but it has become a politicised arm of control. Increasingly internet infrastructure is being used for policy goals — to repress people economically, and physically — we saw it in Kashmir, Myanmar and in the Snowden revelations," says Niels ten Oever, a former Dutch delegate at the ITU.

"For me, the overarching question is: how do we build a public network on privately owned infrastructure? This is the problem we are grappling with. What is the role of the state versus the role of companies?"

In his view, companies design technologies primarily for profit. "The internet is dominated by US companies, all data flows there. So, of course, they want to keep that power," he says. "We are scared of Chinese repression. We are making caricatures of the Chinese in a borderline imperialist-racist way. But the internet governance today is not working. There is room for an alternative."

Wherever our digital future is currently being built, there seems to be global agreement that the time has come for a better version of cyberspace. "I think [some] people would argue that our current model of the internet is deeply flawed, if not broken. At present, there is only one other truly comprehensive and fully realised model out there, China's," wrote Griffiths in *The Great Firewall of China*.

"The risk is that if we fail to come up with a third model — one that empowers users and increases democracy and transparency online, and reduces the powers both of big tech and government security services — then more and more countries will tilt towards the Chinese model, rather than deal with the fallout of the failing Silicon Valley one."

Today, the "Declaration of the Independence of

Cyberspace" — the guiding principle of the internet — is starting to look more and more like a relic. The manifesto, written in 1996 by John Perry Barlow, co-founder of the American non-profit Electronic Frontier Foundation, and a Grateful Dead lyricist, was a call to arms.

"Governments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace, the new home of Mind," starts the document. "On behalf of the future, I ask you of the past to leave us alone. You are not welcome among us. You have no sovereignty where we gather."

That view has now become a throwback to a time before trillion-dollar market capitalisations in the tech industry, critics say. But there is still hope — and possibly a third alternative to our two internets of today.

"What differentiates us from China now is that in the west, the public can still mobilise and have a say. A lot of this now is down to lawmakers to protect democracy in an age of surveillance, whether it's market-driven, or authoritarian-driven," says Zuboff. "The sleeping giant of democracy is finally stirring, lawmakers are waking up, but they need to feel the public at their backs. We need a western web that will offer the kind of vision of a digital future that is compatible with democracy. This is the work of the next decade."

Madhumita Murgia is the FT's European tech *correspondent. Anna Gross is an FT markets reporter. Additional reporting by Yuan Yang and Nian Liu*

Follow @FTMag on Twitter to find out about our latest stories first. Listen to our culture podcast, Culture Call and subscribe on Apple, Spotify, or wherever you listen